EXHIBIT C-5
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 9 ('661 Patent)	U.S. 5,994,917 to Wuidart ("Wuidart")
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:29-40 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to

	observe the operations of the integrated circuit."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-18 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link. In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(b) a source of unpredictable information;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the

	integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ." Figure 1.
(c) a processor:	2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." Figure 1.
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals	2:53-67 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal and a switch-over circuit capable of either the external clock signal or the random clock signal as an input pulse signal of the generator 4 of the internal clock signal. The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the

and said secret during said processing of said quantity;	use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(e) a hardware-	2:17-27 – "According to the invention, it furthermore has a random

implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and	generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	2:21-27 – "The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit. 2:29-40 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits). The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4."

Claim 10 ('661 Patent)	U.S. 5,994,917 to Wuidart
The device of claim 9 wherein said source of unpredictable information is a hardware-implemented random number generator, and wherein said noise production subunit includes a digital-to-analog converter.	2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ." *See also, e.g.*, English abstracts of JP10084223, JP10197610, JP62260406, and JP62082702 (describing including a digital to analog converter in a noise production subunit).

Claim 11 ('661 Patent)	U.S. 5,994,917 to Wuidart
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:29-40 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular,

	the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-18 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a

	serial link. In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." Figure 1.
(d) a noise production	2:17-27 – "According to the invention, it furthermore has a random

system for introducing noise into said measurement of said power consumption.	generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."

Claim 12 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock

	signal . . . ." Figure 1.
(b) a noise processing module for improving the random characteristic of said initial noise; and	2:17-27 – "According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4."
(c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."

Claim 13 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under the control of said processor.	2:21-27 – "The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit. 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external

	exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4."

Claim 14 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to

	observe the operations of the integrated circuit."
(a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(b) an oscillator generating a first clock signal;	Claim 9 – "A circuit for sequencing an integrated circuit, the circuit comprising: a random generator which generates a first secure output clock signal which cannot be monitored externally to the circuit . . . ." *See also* U.S. Patent No. 5,404,402 to Sprunk at, *e.g.*, 3:67-4:13 (describing various types of clock signal sources, including oscillators).
(c) an input interface for receiving a variable amount of power, said	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated

power consumption varying measurably during said performance of said operation;	circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(d) a source of unpredictable information;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ." Figure 1.
(e) a clock decorrelator coupled to said source of unpredictable information for generating a second clock signal from said first clock signal using	2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." Claim 9 – "a switch-over circuit which accepts the first secure output

said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal; and	clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit."
(f) a processor:	2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)."
(i) clocked by said second clock signal,	Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit."
(ii) configured to cryptographically processing said data, and	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit."
(iii) configured to output said cryptographically processed data using said input/output interface.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory

	circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 15 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for

	operations that process confidential data elements." 2:29-40 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-18 – "With an internal sequencing method of this kind, it then

	becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link. In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(b) an input interface for receiving an external clock signal;	2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." Figure 1. *See, e.g.*, W. Rankl and W. Effing, SMART CARD HANDBOOK at 264, John Wiley & Sons, Chichester, 1997 ("The Smart Card's clock is always supplied from outside, so that computational speed is determined entirely externally. This theoretically permits the microprocessor to be run from outside in single step mode, which provides an excellent opportunity for analysis, particularly in the measurement of power consumption and electric potentials in the chip.").
(c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(d) a source of	1:54-64 – "An embodiment of the present invention is directed to an

unpredictable information;	integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ." Figure 1.
(e) a clock decorrelator coupled to said source of unpredictable information for generating an internal clock signal from said external clock signal using said unpredictable information, such that said internal clock signal cannot be reliably predicted from said external clock signal; and	2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:53-67 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal and a switch-over circuit capable of either the external clock signal or the random clock signal as an input pulse signal of the generator 4 of the internal clock signal. The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure

	output clock signal to the integrated circuit." Claim 20 – "A system for sequencing an integrated circuit, the system comprising: a first clock signal which is provided externally to the integrated circuit by an external means; means for internally generating a second clock signal; and means for providing a third clock signal to the integrated circuit based upon the first clock signal and second clock signal, wherein the third clock signal is provided according to an operation performed by the integrated circuit."
(f) a processor:	2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)."
(i) clocked by said internal clock signal,	2:20-27 – "The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:53-67 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal and a switch-over circuit capable of either the external clock signal or the random clock signal as an input pulse signal of the generator 4 of the internal clock signal. The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." Claim 9 – "a switch-over circuit which accepts the first secure output

	clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit." Figure 1.
(ii) configured to cryptographically processing said data, and	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 2:64-67 – "Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(iii) configured to output said cryptographically processed data using said input/output interface.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external

	synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 16 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The device of claim 15 wherein said clock decorrelator comprises a clock skipping module which selects a subset of the cycles of said external clock signal to use as said internal clock signal based on said unpredictable information.	Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit." *See also* claims 20, 21.

Claim 17 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The device of claim 15 wherein said source of unpredictable information comprises a hardware random number generator.	2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ."

Claim 18 ('661 Patent)	U.S. 5,994,917 to Wuidart
The device of claim 15 further comprising a monitor for detecting a clock fault in said external clock signal and preventing said processor from processing said quantity if said clock fault is detected.	1:18-25 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit. A disturbing action by parasites would be one way of carrying out fraudulent activity." *See also* U.S. Patent Number 5,249,294 to Griffin et al. at, for example, 2:30-36 and 4:40-5:43.

Claim 19 ('661 Patent)	U.S. 5,994,917 to Wuidart
The device of claim 15 wherein said clock decorrelator is selectively operable under the control of said processor.	2:21-27 – "The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit. 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4."

Claim 20 ('661 Patent)	U.S. 5,994,917 to Wuidart
The device of claim 15 wherein said clock decorrelator is selectively operable such that said clock decorrelator is disabled when data is being transferred across said input/output interface and enabled during said	1:59-64 – "Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:21-27 – "The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being

cryptographic processing operation.	done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit. 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 21 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The device of claim 15 further comprising a noise production system connected to said processor for introducing noise into said measurement of the power consumption by consuming a random amount of power during said cryptographic prosing operation.	2:17-27 – "According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time

	d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."

Claim 22 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards."

Claim 29 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:29-40 – "This circuitry 5 is not shown in detail in the figure, but it

	typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(b) receiving a quantity to be cryptographically processed, said quantity being	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards."

representative of at least a portion of a message;	2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-18 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link. In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-27 – "According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al. The two

	clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:14-19 – "FIG. 1 shows a block diagram of an integrated circuit 1 enabling the implementation of the invention. The integrated circuit 1 has an input to receive an external clock signal CK-ext. According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external

	synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 30 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ." Figure 1.
(b) improving the random characteristic of said initial noise; and	2:17-27 – "According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-

	over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4."
(c) varying said power consumption based on said improved initial noise.	2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."

Claim 31 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-

	intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(b) generating a first clock signal;	Claim 9 – "A circuit for sequencing an integrated circuit, the circuit comprising: a random generator which generates a first secure output clock signal which cannot be monitored externally to the circuit . . . ."
(c) receiving data to be cryptographically processed, said data being representative of at least a portion of a	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it

message;	typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(d) generating unpredictable information;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock

	signal . . . ."
(e) generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal;	2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit."
(f) processing said data using said second clock signal; and	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit."
(g) outputting said cryptographically processed quantity to a recipient thereof.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose

	the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 32 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." 1:36-46 – "However, it has been discovered that such structures, while they make it possible to prevent the disturbing of the internal operation of an integrated circuit, do not however make it possible to prevent another type of fraud, namely the observation of the behavior of the integrated circuit. Since the internal clock signal is based on the external clock signal, this external clock signal may be used as a synchronization signal. This would, for instance, enable an ill-intentioned individual in particular to obtain confidential data or even information by which the individual could reconstitute the program

	performed by the integrated circuit." 1:59-60 – "Preferably, the random clock signal will be used for operations that process confidential data elements." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit."
(b) receiving an external clock signal;	2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." Figure 1. *See, e.g.,* W. Rankl and W. Effing, SMART CARD HANDBOOK at 264, John Wiley & Sons, Chichester, 1997 ("The Smart Card's clock is always supplied from outside, so that computational speed is determined entirely externally. This theoretically permits the microprocessor to be run from outside in single step mode, which

	provides an excellent opportunity for analysis, particularly in the measurement of power consumption and electric potentials in the chip.").
(c) receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."
(d) generating unpredictable information;	1:54-64 – "An embodiment of the present invention is directed to an integrated circuit which internally generates a random clock signal, which allows the integrated circuit to use either the external clock signal or the random clock signal according to the instruction to be performed by the integrated circuit. Preferably, the random clock signal will be used for operations that process confidential data elements. Also, in another embodiment of the invention, the integrated circuit can use the random clock signal by default so that the external clock signal is switched over only for operations

	requiring external synchronization." 2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ."
(e) generating an internal clock signal from said external clock signal using said unpredictable information, such that said external clock signal cannot be reliably predicted from said internal clock signal;	2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit." Claim 20 – "A system for sequencing an integrated circuit, the system comprising: a first clock signal which is provided externally to the integrated circuit by an external means; means for internally generating a second clock signal; and means for providing a third clock signal to the integrated circuit based upon the first clock signal and second clock signal, wherein the third clock signal is provided according to an operation performed by the integrated circuit."
(f) processing said data using said internal clock signal; and	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 1:18-23 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit." Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a

	clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit."
(g) outputting said cryptographically processed quantity to a recipient thereof.	1:7-9 – "The present invention relates to a method and apparatus for sequencing an integrated circuit, and can be applied to integrated circuits designed for chip cards or circuit boards." 2:29-34 – "This circuitry 5 is not shown in detail in the figure, but it typically has memory circuits in which there are stored, in particular, the application program and confidential data elements (an identification code for example) and means to manage the external exchanges and these memory circuits (processor, microcontroller or other circuits)." 2:58-67 – "The switch-over circuit thus makes it possible to impose the random clock signal as an input pulse signal for operations processing confidential data elements (contained in the memory circuits of the circuitry 5). Also, the switch-over circuit enables the use of the external clock signal for operations requiring external synchronization. Therefore, the confidential data elements contained in the integrated circuit are protected from fraudulent activity since it is no longer possible to find any external synchronization in order to observe the operations of the integrated circuit." 3:7-12 – "With an internal sequencing method of this kind, it then becomes impossible to find an external synchronization. The only operations of the integrated circuit that will be synchronized with the external clock signal will be those relating to the transmission of data elements with an external system, for example transmission by a serial link." 3:13-18 – "In practice, when the integrated circuit carries out the program and when it reaches instructions corresponding to a transmission (sending or receiving) with an external system, it activates the command K(K=1) to temporarily switch the external clock signal to the generator circuit input."

Claim 33 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The method of claim 32 wherein said step of generating said internal clock signal comprises a	Claim 9 – "a switch-over circuit which accepts the first secure output clock signal of the random generator and an external clock signal and switches between the first secure output clock signal and the external clock signal to provide a second secure output clock signal; and a

step of selecting a subset of the cycles of said external clock signal to use as said internal clock signal based on said unpredictable information.	clock signal generator circuit which accepts the second secure output clock signal of the switch-over circuit and provides a third secure output clock signal to the integrated circuit." *See also* claims 20, 21. *See also* U.S. Patent No. 5,404,402 to Sprunk at, *e.g.*, 2:26-3:8; Posting of Jim Bell to sci.crypt newsgroup, http://groups.google.com/group/sci.crypt/msg/485abca33cc29703?dmode=source&hl=en (December 24, 1995), last visited November 17, 2006.

Claim 34 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The method of claim 32 wherein said step of generating unpredictable information comprises a step of generating a random number.	2:17-19 – "According to the invention, [the integrated circuit 1] furthermore has a random generator 2 which provides a random clock signal CK-al." 2:53-55 – "An integrated circuit according to the invention, comprises a random generator capable of providing a random clock signal . . . ."

Claim 35 ('661 Patent)	**U.S. 5,994,917 to Wuidart**
The method of claim 32 further comprising a step of monitoring for a clock fault in said external clock signal and a step of preventing said processor from outputting said cryptographically processed quantity if said clock fault is detected.	1:18-25 – "For chip card applications, circuit board applications, or for any other application requiring high operating security, it is imperative to have the ability to prevent a situation where the presence of parasites on the external clock signal could disturb the internal clock signal and modify the operation of the integrated circuit. A disturbing action by parasites would be one way of carrying out fraudulent activity." *See also* U.S. Patent Number 5,249,294 to Griffin et al. at, for example, 2:30-36 and 4:40-5:43.

Claim 36 ('661 Patent)	U.S. 5,994,917 to Wuidart
The method of claim 32 further comprising a step of introducing noise into said measurement of the power consumption.	2:17-27 – "According to the invention, it furthermore has a random generator 2 which provides a random clock signal CK-al. The two clock signals CK-ext and CK-al are applied to two inputs of a switch-over circuit 3. The circuit 3 is capable of switching either of the clock signals over to an input E of a circuit for the generation of an internal clock signal CK-in, this switch-over being done according to the level of a binary command K which may be 0 or 1. This internal clock signal CK-in is applied to the circuitry of the integrated circuit." 2:35-40 – "The switch-over circuit 3 receives the binary switch-over command K from circuitry 5. Depending on whether its logic state is low or high, this command enables either the random clock signal or of the external clock signal to be switched over to the input E of the clock signal generator circuit 4." 2:41-52 – "This generator circuit 4 provides an output signal whose pulses are stabilized 15 in time. Typically, and as shown in FIG. 2, the detection of a leading edge on the input E makes the output signal go from a low state to a high state during a calibrated period of time d1, and then the output signal goes back to the low state for at least a determined period of time d2. It is only at the end of this period d2 that the generation circuit can respond to a new pulse at its input E. A generation circuits, such as the circuits described in the patent application No. FR 2 708 809 may be an appropriate generation circuit which could be used in the present invention."